BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-041281
(43)Date of publication of application : 08.02.2002

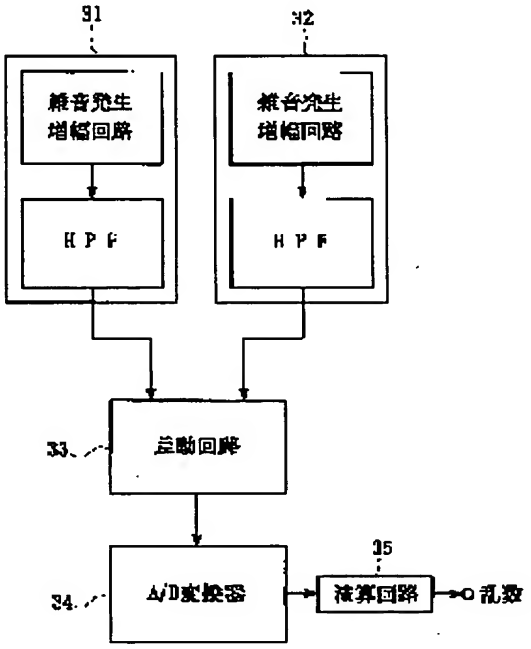
(51)Int.Cl. G06F 7/58
H03K 3/84

(21)Application number : 2000-222525
(22)Date of filing : 24.07.2000

(71)Applicant : UNIV NIIGATA
(72)Inventor : SAITO YOSHIAKI

(54) RANDOM NUMBER GENERATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method to generate more perfect random numbers that have no periodicity of 1/f characteristics based on the noises being generated from a noise source that has 1/f characteristics.
SOLUTION: The noise generated from a diode that has the 1/f characteristics is amplified, and the differential of the noises outputted from the first noise generation circuit 31 and the second noise generation circuit 32 that eliminate the hum with high path filters is taken by a differential circuit 33 and the noise that has no periodicity is taken out, and '1' and '0' are generated through the comparison of a threshold level and binary numbers generated from digital signals obtained through the A/D conversion of the above noises. The threshold level is adjusted in order to make the appearance probability of these '1' and '0' closer to 0.5. Delimiting '1' and '0' that are obtained in above manner in each specified period generates random numbers. The period can be changed in accordance with the random numbers generated.



LEGAL STATUS

[Date of request for examination] 24.07.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－41281
（P2002－41281A）
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ	５Ｊ０４９
Ｈ０３Ｋ　3/84		Ｈ０３Ｋ　3/84	Ｚ	

審査請求　有　　請求項の数８　ＯＬ　（全　５　頁）

(21)出願番号　特願2000－222525(P2000－222525)

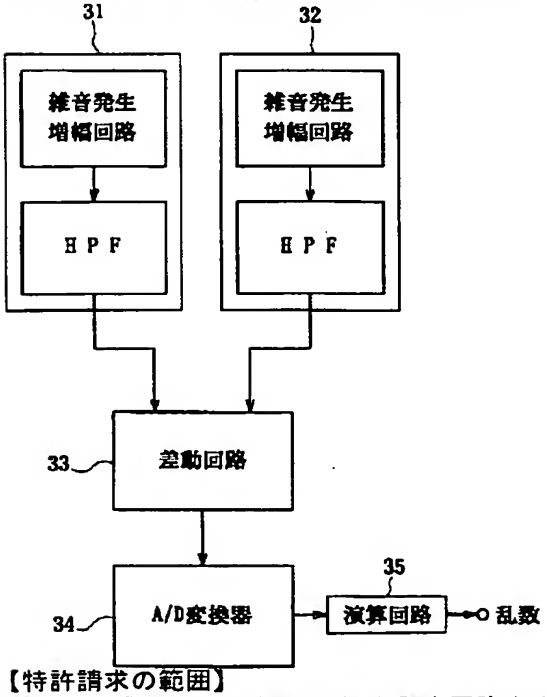
(22)出願日　平成12年７月24日(2000.7.24)

(71)出願人　596133441
新潟大学長
新潟県新潟市五十嵐２の町8050番地
(72)発明者　斉藤　義明
新潟県新潟市五十嵐１の町7794番地20
(74)代理人　100059258
弁理士　杉村　暁秀　（外２名）

Ｆターム(参考)　5J049 AA13 AA20 CA03

(54)【発明の名称】　乱数発生方法

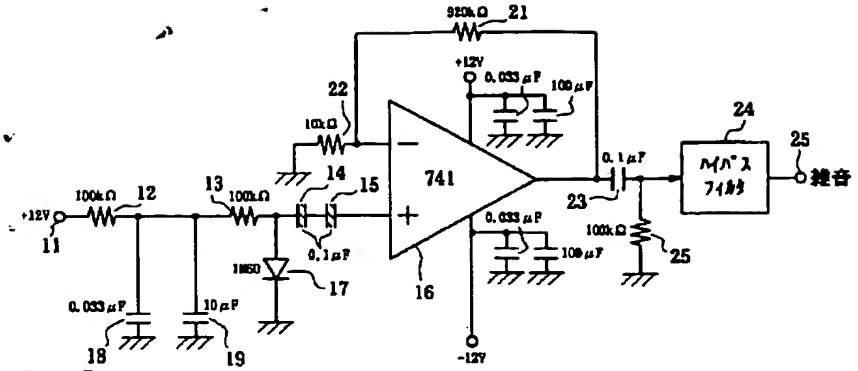
(57)【要約】
【課題】１／f特性を有する雑音発生源から発生される雑音に基づいて、１／f特性による周期性を持たないより完全な乱数を発生させる方法を提供する。
【解決手段】１／f特性を有するダイオードから発生される雑音を増幅し、ハイパスフィルタでハムを除去する第１および第２の雑音発生回路31および32から出力される雑音の差動を差動回路33で取って周期性を持たない雑音を取り出し、この雑音をA／D変換して得られるディジタル信号をまとめて2進数を生成し、その大きさとスレシュホールドレベルとの比較で「１」および「０」を生成する。これら「１」および「０」の出現確率が０．５に近づくようにスレシュホールドレベルを調整する。このようにして得られる「１」、「０」を所定の期間毎に区切って乱数を生成する。この期間を生成した乱数にしたがって変化させてもよい。



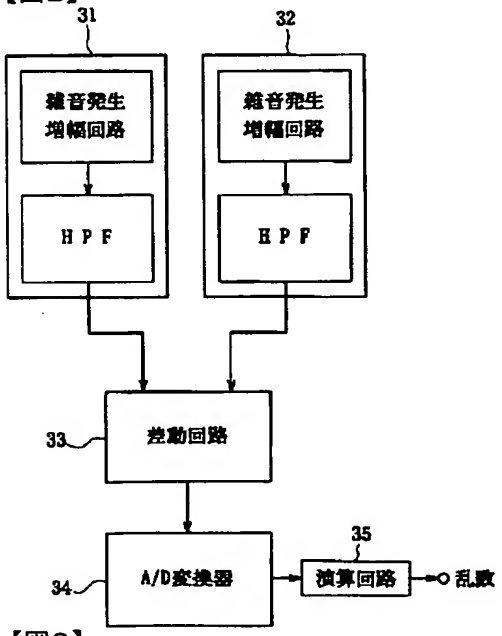
【特許請求の範囲】
【請求項１】第１および第２の雑音発生回路出力される雑音の差動を差動回路で取り、この差動回路から出力される信号から周期性を持たない乱数を発生することを特徴とする乱数発生方法。

【請求項2】前記差動回路から出力される信号を、アナログ－ディジタル変換回路でディジタル信号に変換し、このアナログ－ディジタル変換回路から出力されるディジタル信号をそのまま数値として乱数を生成することを特徴とする請求項1に記載の乱数発生方法。
【請求項3】前記アナログ－ディジタル変換回路から出力されるディジタル信号の区切りを変化させることを特徴とする請求項2に記載の乱数発生方法。
【請求項4】前記アナログ－ディジタル変換回路から出力されるディジタル信号の1ビットまたは複数ビットをまとめて1個の数値とし、この数値を予め設定されたスレシュホールドレベルと比較し、数値がこのスレシュホールドレベルを越えるか否かに応じて2進数の「0」および「1」の一方および他方を割り当てて乱数を発生させることを特徴とする請求項2に記載の乱数発生方法。
【請求項5】前記数値がスレシュホールドレベルを越えるか否かに応じて割り当てられる2進数の「0」および「1」の出現確率を検出し、これらの出現確率が所定の値となるように前記スレシュホールドレベルを調整することを特徴とする請求項4に記載の乱数発生方法。
【請求項6】前記2進数の「0」および「1」の出現確率がそれぞれ0．5に近づくように前記スレッシュホールドレベルを調整することを特徴とする請求項5に記載の乱数発生方法。
【請求項7】前記2進数の「0」および「1」の出現確率がそれぞれ0．5に近づくように2進数の「0」および「1」の出現確率を検出する期間を調整することを特徴とする請求項5に記載の乱数発生方法。
【請求項8】前記2進数の「0」および「1」の出現確率を検出する期間を、発生させた乱数に基づいて設定することを特徴とする請求項5または6に記載の乱数発生方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、乱数発生方法、特に周期性を実質的に持たない乱数を発生させる方法に関するものである。
【0002】
【従来の技術】完全に無秩序でかつ全体としては出現頻度が等しくなる乱数は、社会現象や物理現象の数値シミュレーションなどに広く利用されている。また、乱数を用いて暗号化することも提案されている。例えば、電子商取引や、電子カルテや遠隔医療に伴う個人情報の保護など医療の分野においては暗号化に対する需要が高まっている。
【0003】従来、乱数を発生させる一般的な方法は、コンピュータのソフトによって発生させるものである。しかしながら、コンピュータによって乱数を発生させる場合には、数式に基づいて乱数を発生させているので何らかの周期性または規則性を有し、完全な乱数とはならない欠点がある。したがって、このようにコンピュータから発生させた乱数を用いて秘密にしておきたいデータを暗号化した場合、簡単に解読されてしまい、個人情報の十分な保護が図れないという問題がある。
【発明が解決しようとする課題】
【0004】このような欠点を解消しようとして、抵抗やダイオードなどの電気素子が発生する雑音から乱数を発生させることが提案されている。しかしながら、例えば抵抗が発生する雑音は、いわゆる1／f特性を有している。すなわち、周波数の低い雑音の振幅は高く、周波数の高い雑音の振幅は低くなるので、雑音の振幅に応じて2値化された信号から乱数を生成する場合には、1／f特性によって乱数が周期性を持ってしまうという問題があり、規則性を持たない乱数を発生させることができない欠点がある。抵抗以外の雑音発生源、例えばダイオードから発生される雑音も1／f特性を有しているので、それから発生される乱数も周期性を持つことになる。
【0005】したがって本発明の目的は、上述した従来の欠点を除去し、1／f特性を有する雑音から周期性や規則性を持たないほぼ完全な乱数を発生させる方法を提供しようとするものである。
【0006】
【課題を解決するための手段】本発明による乱数発生方法は、第1および第2の雑音発生回路出力される1／f特性を有する雑音の差動を差動回路で取り、この差動回路から出力される信号から1／f特性に基づく周期性を持たない乱数を発生することを特徴とするものである。
【0007】このような本発明による乱数発生方法によれば、第1および第2の雑音発生回路からそれぞれ出力される雑音は1／f特性を有していても、これらの雑音の差動を差動回路で取ると、発生頻度の高い周波数の高い雑音が相殺される可能性は、発生頻度の低い雑音が相殺される可能性よりも高くなり、どの周波数でもほぼ一定の出現確率となるので、差動回路から出力される信号からは1／f特性が除去され、したがってこのような信号から生成される乱数は周期性を持たないものとなる。
【0008】本発明による乱数発生方法の好適な実施例においては、前記差動回路から出力される信号を、アナログ－ディジタル変換回路でディジタル信号に変換し、このアナログ－ディジタル変換回路から出力されるディジタル信号をそのまま数値として乱数を生成する。この場合、前記アナログ－ディジタル変換回路から出力されるディジタル信号の区切りを変化させることによって種々の乱数を発生させることができる。
【0009】本発明による乱数発生方法の他の好適な実施例においては、前記アナログ－ディジタル変換回路から出力されるディジタル信号の1ビットまたは複数ビットをまとめて1個の数値とし、この数値を予め設定されたスレシュホールドレベルと比較し、数値がこのスレシュホールドレベルを越えるか否かに応じて2進数の「0」および「1」の一方および他方を割り当てて乱数を発生させる。この場合、前記数値がスレシュホールドレベルを越えるか否かに応じて割り当てられる2進数の「0」および「1」の出現確率を検出し、これらの出現確率が所定の値、例えばそれぞれ0．5となるように前記スレシュホールドレベルを調整するのが好適である。或いは、2進数の「0」および「1」の出現確率を検出する期間を調整することもできる。
【0010】
【発明の実施の形態】図1は本発明による乱数発生方法を実施するための雑音発生回路の一例を示す回路図である。本例では、雑音源としてダイオードを用いるものであるが、その雑音は小さいので増幅して使用すると共に直流電源に混入している恐れのある周期性のハムを除去している。12ボルトの直流電圧が印加される入力端子11を、抵抗12、13および電解コンデンサ14、15を経て増幅器16の正入力端子へ接続する。抵抗13と電解コンデンサ14との接続点を、雑音発生用ダイオード17のアノードに接続し、このダイオードのカソードを接地する。また、抵抗12と13との接続点と大地との間には、コンデンサ18および19を並列に接続する。
【0011】増幅器16の出力端子を帰還抵抗21および22を経て接地し、これらの抵抗の接続点を増幅器の負入力端子へ接続する。また、増幅器16の出力端子を結合コンデンサ23を経てハイパスフィルタ24へ接続する。結合コンデンサ23とハイパスフィルタ24の入力端子との間の接続点を抵抗25を経て接地する。このようにハイパスフィルタ24に通すことにより、雑音に混入されたハムなどの周期性成分を除去する。したがって、ハイパスフィルタ24に接続された出力端子26には、ダイオードで生成され、増幅器で増幅された雑音が出力されることになるが、この雑音は1／f特性を有するものである。上述した抵抗、コンデンサの具体的な値を図面に示したが、本発明はこのような数値に限定されるものでないことは勿論である。

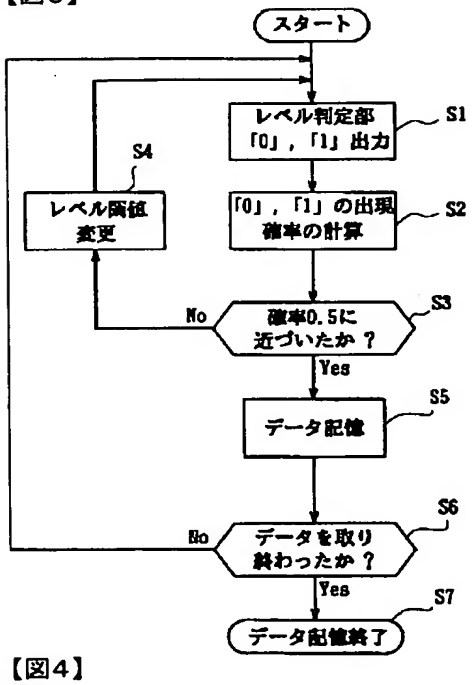
【0012】図2は本発明による乱数発生方法を実施する乱数発生回路の全体の構成を示すフロック図である。各々が図1に示した構成を有する第1および第2の雑音発生回路31および32から出力される1／f特性を有する雑音を、差動回路33へ供給してこれらの雑音の差動を取る。第1および第2の雑音発生回路31および32から出力される雑音は1／f特性を有しており、周波数の低い雑音の振幅は大きく、周波数の高い雑音の振幅は小さい。したがって、このような1／f特性を有する雑音をアナログーディジタル変換する場合、小さいディジタル信号は大きなディジタル信号よりも出現確率が高くなり、周期性を持つことになる。したがって、このようなディジタル信号から乱数を生成すると、その乱数も周期性を持つことになり、完全な乱数を生成することができない。
【0013】本発明においては、このような周期性を抑圧するために、第1および第2の雑音発生回路31および32から出力される雑音を差動回路33へ供給してこれらの雑音の差動を取る。このようにそれぞれが1／f特性を有する雑音の差動を取ると、周波数が高い雑音が相殺除去される確率は、周波数が低い雑音が相殺除去される確率よりも高くなるので、周波数の高い雑音の出現確率は、周波数の低い雑音の出現確率よりも高い割合で低減することになり、どの周波数においてもほぼ一定の出現確率となる。したがって、差動回路33から出力される雑音に基づいて乱数を生成することによって1／f特性の影響を除去し、周期性のない乱数を発生させることができる。
【0014】本例においては、差動回路33から出力される雑音を、アナログーディジタル変換回路34へ供給してディジタル信号に変換し、このディジタル信号を演算回路35へ供給する。演算回路35においては、アナログーディジタル変換回路33から出力されるディジタル信号をそのまま出力することによってディジタル乱数を生成することができ、ディジタル変換された数値の区切りを変えることによって別の乱数を発生させることができるが、本例では演算回路35において、1ビットまたは複数ビットをまとめて1個の数値とし、その値を予め決めたスレシュホールドレベルと比較して2進数の「0」および「1」ビットより成る乱数を生成する。
【0015】上述したように演算回路35においてスレシュホールドレベルと比較して生成される「0」および「1」ビットをそのまま乱数とすると、これらのビットの出現確率は制御されていないので、完全な乱数とはならない場合もある。そこで、本例では、演算回路35において、「0」ビットと「1」ビットの出現確率を計算し、これらの出現確率が0．5となるようにスレシュホールドレベルを調整するようにしている。
【0016】図3は、上述したように、「0」ビットと「1」ビットの出現確率を計算し、これらの出現確率が0．5となるようにスレシュホールドレベルを調整するようにして乱数を発生させるプロセスを示すフローチャートである。ステップS1において、アナログーディジタル変換回路33から出力されるディジタル信号の大きさを所定のスレシュホールドレベルと比較し、スレシュホールドレベル以上の場合には「1」ビットを出力し、スレシュホールドレベルに達しない場合には「0」ビットを出力する。次に、ステップS2において、所定の期間に亘って、「1」ビットおよび「0」ビットの出現確率を計算する。
【0017】さらにステップS3において、計算された「1」ビットおよび「0」ビットの出現確率が0．5に近づいたか否かを判定する。ここで、出現確率が0．5に近づかないと判断される場合には、ステップS4において、スレシュホールドレベルを変更する。この場合、「1」ビットの出現確率が「0」ビットの出現確率よりも高い場合には、スレシュホールドレベルを上げ、反対に「1」ビットの出現確率が「0」ビットの出現確率よりも低い場合には、スレシュホールドレベルを下げるように変更する。
【0018】このような操作を繰り返すことによって、「1」ビットの出現確率と「0」ビットの出現確率が共に0．5に近づいたことが判定された場合には、ステップS5において、これらのビットより成る乱数データを記録し、ステップS6において必要な個数の乱数データを取り終わったことが確認されたら、ステップS7において乱数データの記録を終了する。
【0019】図4は本発明による方法によって発生させた乱数の分散状態の実験結果を示すものである。本例では、生成した2進数を16ビット毎に区切り、最初の8ビットの数値を縦軸の座標とし、残りの8ビットの数値を横軸の座標として座標位置を求めた3000点をプロットしたものである。図5は雑音発生回路を1組しか用いていない従来の乱数発生方法で発生させた乱数を同様にプロットしたものである。本発明によれば、図4に示すように3000点は全体に均一に分散し、したがって発生させた乱数は雑音発生源の1／f特性による周期性を持たないことがわかる。これに対し、図5に示す従来の方法では、或る領域に点が集中し、絣状の模様が現れ、乱数は周期性を有することがわかる。
【0020】本発明は上述した実施例にのみ限定されるものではなく、幾多の変更や変形が可能である。例えば、上述した実施例においては1／f特性を有する雑音を発生する雑音発生源をダイオードとしたが、1／f特性を有する抵抗のような他の電気素子とすることもできる。
【0021】上述したように本発明による乱数発生方法によれば、それぞれが1／f特性を有する2つの雑音発生回路から出力される雑音の差動を差動回路で取ることによって1／f特性を抑圧した信号を得ることができるので、周期性のない乱数を発生させることができる。このような乱数を用いて暗号を生成すれば、規則性がないので最も解読されにくくなり、情報化社会のセキュリティの向上に大きく貢献することができ、その社会的な意義は非常に大きなものである。さらに、2進数「0」と「1」の出現確率を調整することによって生成される乱数の性質を調整することもできるので、それにより作られる暗号はさらに解読され難いものとなる。
【図面の簡単な説明】
【図1】本発明による乱数発生方法に用いる雑音発生回路の一例の構成を示す回路図である。
【図2】図1に示した雑音発生回路を2つ用いて本発明による乱数発生方法を実施する回路の一例の構成を示すブロック図である。
【図3】図2に示す乱数発生回路の動作を説明するためのフローチャートである。
【図4】本発明による乱数発生方法によって発生させた乱数の分布状態を示すグラフである。
【図5】従来の乱数発生方法によって発生させた乱数の分布状態を示すグラフである。
【符号の説明】
16 増幅器、17 ダイオード、24 ハイパスフィルタ、31、32第1および第2の雑音発生回路、33 差動回路、34 アナログーディジタル変換回路、35 演算回路
【図1】


920kΩ
21
+12V
0.033μF
100μF
22
10kΩ
741
24
25
雑音
0.1μF
23
ハイパス
フィルタ
100kΩ
12
13
100kΩ
14
15
+12V
11
0.1μF
1N60
17
0.033μF
10μF
18
19
16
-12V
100kΩ
25

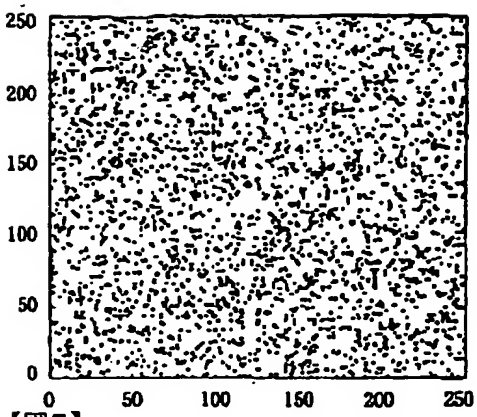
【図2】


31
32
雑音発生
増幅回路
雑音発生
増幅回路
H P F
H P F
33
差動回路
35
34
A/D変換器
演算回路
乱数

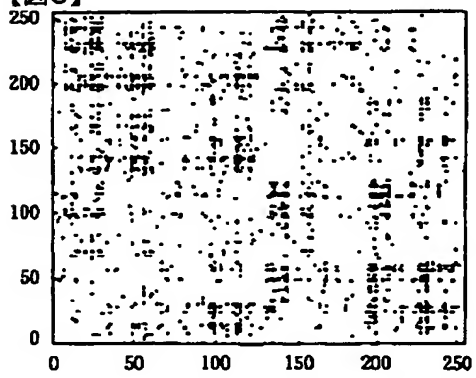
【図3】


スタート
レベル判定部
「0」，「1」出力
S1
S4
レベル閾値
変更
「0」，「1」の出現
確率の計算
S2
No
確率0.5に
近づいたか？
S3
Yes
データ記憶
S5
No
データを取り
終わったか？
S6
Yes
データ記憶終了
S7

【図4】


250
200
150
100
50
0
0
50
100
150
200
250

【図5】


250
200
150
100
50
0
0
50
100
150
200
250